RAPID7

Medium Enterprise Energy & Utilities Company

Introduction

This case study of a medium enterprise energy & utilities company is based on a February 2022 survey of Rapid7 Managed Detection and Response (MDR) Services & Solutions customers by TechValidate, a 3rd-party research service. The profiled company asked to have their name blinded to protect their confidentiality.

"

"MDR has strengthened our security posture immensely. Prior to having MDR monitor our environment, only basic alerting was setup on individual systems that could not paint the whole picture. Many of these alerts would be false positives and would be ignored. Now that we have an entire team watching the entire environment, we know any alert that comes from MDR is worth investigating! "

"Without Rapid7 MDR, our team would not be able to sleep well at night!"

Challenges

The business challenges that led the profiled company to evaluate and ultimately select Rapid7 Managed Detection and Response (MDR) Services & Solutions:

- They decided to adopt a managed detection and response solution because:
  - They had no existing D&R Program
  - They didn't have a large enough team to do it in-house
  - They didn't have the right technology
  - They needed expert support and guidance
- Prior to implementing Rapid7 MDR, they had approximately 1 dedicated FTEs as part of their organization's in-house cybersecurity team.

Use Case

- The criteria that was most important in their decision to select Rapid7 MDR was:
  - Team augmentation
  - Containment/Incident response
  - Visibility and reporting
  - Cybersecurity expertise

Results

- The aspects of Rapid7 MDR most impactful to their organizations' security success were:
  - 24 × 7 × 365 SOC team
  - Access to the XDR technology the MDR SOC uses
  - Ability to pivot to engage Rapid7 in Incident Response if breached
- They said "Our detection and response program has substantially improved since partnering with Rapid7 MDR."
- How they rate the following capabilities based on experience with Rapid7 MDR:
  - SOC Expertise: Excellent
  - Technology: Excellent
  - Threat detection: Excellent
  - Incident Response: Excellent
  - Reporting: Excellent
  - Customer Advisor Guidance: Excellent
- Since we've implemented Rapid7 MDR, our team has:
  - Spent less time doing investigations
  - Improved their Mean Time To Detect (MTTD)
  - Improved their Mean Time To Respond (MTTR)
  - Received less false positives
  - Had more time to focus on other security initiatives
  - Had more time to focus on professional development/skills
  - Improved their coverage outside the 5×8 work week
  - Have improved our overall security posture
  - Have been able to engage more with the business

Company Profile

The company featured in this case study asked to have its name publicly blinded because publicly endorsing vendors is against their policies.

TechValidate stands behind the authenticity of this data.

Company Size:
Medium Enterprise

Industry:
Energy & Utilities

About Rapid7 Managed Detection and Response (MDR) Services & Solutions

Rapid7 is advancing security to accelerate innovation. Learn how the MDR service provides round-the-clock expert monitoring to defend against threats and stop attackers in their tracks at rapid7.com/mdr.

Learn More:

⬁ Rapid7